UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

INTERWORK KOREA CO. LTD.,

Plaintiff/Counterclaim-Defendant,

v.

LASHIFY, INC.,

Defendant/Counterclaim-Plaintiff.

Case No. 25-cv-2752 (VSB)

STIPULATION AND ORDER ON PROTOCOL REGARDING DISCOVERY AND PRODUCTION OF ELECTRONICALLY STORED INFORMATION

Pursuant to Fed. R. Civ. P. 26, Plaintiff/Counterclaim-Defendant Interwork Korea Co. Ltd. ("**IWK**") and Defendant/Counterclaim-Plaintiff Lashify, Inc. ("**Lashify**") (collectively, the "**Parties**" and each a "**Party**"), by their respective counsel in this action, stipulate and agree that the following discovery protocol shall govern the search and production of electronically stored information ("**ESI**"), and the production of paper documents in electronic form, in this matter (the "**ESI Protocol**"). This ESI Protocol shall govern the production of documents that are relevant and responsive to formal Requests for Production of Documents and, if applicable, Interrogatories, as well as documents that otherwise need to be produced under applicable law.

(1) <u>Competence</u>

Counsel certify that they are sufficiently knowledgeable in matters relating to each of their client's technological systems to competently discuss issues relating to electronic discovery, or have involved someone competent to address these issues on their behalf.

(2) <u>Preservation of ESI & Inaccessible Data</u>

Each Party has disclosed a list of data sources of which each Party is presently aware, if any, likely to contain discoverable ESI (by type, date, custodian, electronic system or other criteria sufficient to specifically identify the data source) that a Party asserts is not reasonably accessible under Fed. R. Civ. P. 26(b)(2)(B). This list is included as **Exhibit A** to this ESI Protocol.

The Parties acknowledge that they have a common law obligation to take reasonable and proportional steps to preserve discoverable information in the Party's possession, custody or control. With respect to preservation of ESI, the Parties agree as follows:

(a) Absent a showing of good cause by the requesting Party, the Parties shall not be required to modify the procedures used by them in the ordinary course of business to back-up and archive data; provided, however, that the Parties shall preserve all discoverable ESI in their possession, custody or control, and that the Parties shall not take the position that data backed up or archived any time after November 1, 2020 has become inaccessible or unavailable due to burden or expense.

(b) All Parties shall supplement their disclosures in accordance with Rule 26(e) with discoverable ESI responsive to a particular discovery request or mandatory disclosure where that data is created after a disclosure or response is made (unless excluded under (c) below).

(c) Absent a showing of good cause by the requesting Party, the following categories of ESI need not be preserved:

1. Data contained on backup tapes or similar back up data contained on any other media.
2. Deleted, fragmented, or other data only accessible by forensics.
3. Random access memory ("**RAM**"), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system.
4. Online access data such as temporary internet files, history, cache, cookies, and the like.

5. Server, system, or network logs.

6. Data remaining from “legacy” systems no longer in use that is unintelligible on the systems in use.

7. Encrypted data/password-protected files, where the key or password cannot be ascertained after reasonable efforts.

8. Voicemail, except for voicemail, if any, that is converted to text and/or audio file and forwarded to a custodian’s email account.

(3) Search & Review

The Parties have discussed methodologies or protocols for the search and review of ESI, as well as the disclosure of techniques to be used and the foregoing will apply to the searches of the locations described in Section 4 below.

The Parties will apply the date range of November 1, 2020 to the present, to the custodial data and other data sources outlined in **Exhibits B** and **C**. The Parties will then apply certain search terms, which shall be negotiated and agreed upon by the Parties (the “Search Terms”), to search those data sources. The Parties agree not to run search terms directly within the native data sources, but rather to apply the search terms after the data sources are collected and properly processed for further review. This will ensure email attachments and other native file types (e.g., Adobe PDFs) are indexed for proper searching, in addition to any password protected or encrypted files to be identified and properly accessed or decrypted for similar handling. After applying the Search Terms, the Parties will then manually review the results to determine which documents, if any, are responsive, relevant, and non-privileged.

(4) Production

(a) Sources of ESI & Data Locations to be Searched

Each Party has supplied a list of custodians most likely to have discoverable ESI in each Party's possession, custody, or control. Those custodians have been identified in **Exhibit B** to this ESI Protocol.

The Parties agree that, subject to the limitations set forth below, the following data locations will be searched for the custodians identified in **Exhibit B** ("Custodians") using the searching methods described in Section 6 and below.

If, after the execution of this ESI Protocol, a Party identifies an individual in a supplemental Rule 26 disclosure who is not already identified as a Custodian in **Exhibit B** hereto, the Parties will discuss in good faith whether that individual should be included as a Custodian and whether the disclosing Party shall search data locations not already searched for that Custodian to identify documents responsive to Requests for Production of Documents.

1. Email

The Parties will use the Search Terms to search for responsive e-mail messages (and attachments thereto), calendar entries, voicemails (to the extent electronically stored in email), and all other electronic files of any type stored in the mail folder(s) or files on their respective current active mail servers or e-mail cloud provider, for the Custodians identified at **Exhibit B**, to the extent such data exists. The Parties will search all folders and subfolders, including without limitation, the "Deleted Items" folder, the "Sent" folder, as well as the "Inbox." To the extent that either Party utilizes a vaulting or similar system to archive e-mails (*e.g.*, Symantec Vault), and to the extent that those e-mails are located on a server that is different from the Party's current active mail server, that server will also be searched for responsive e-mails.

Subject to the foregoing, neither Party shall be required to search or produce data from the contacts, address book, or similar items. Also, .OST files, .PST files and/or any other similar type of local copies, archives or replicas stored in network locations or locally on work stations do not need to be searched unless a Party knows or has reason to believe that the file contains relevant, responsive, non-duplicative data.

2. Collaboration Data, Electronic Desktop, or Laptop Messaging Services

The Parties will use the Search Terms to search for responsive electronic messages (and attachments thereto), including SMS, text message, Teams, Skype, Google Chat, Slack, WhatsApp, Signal, Discord, or any other chat applications, for the Custodians identified at **Exhibit B**, to the extent such data exists. The Parties will identify and provide channel information, including ownership and participants for each channel, and search all folders and subfolders within the collaboration or messaging platform.

3. Network Drive

A custodian's "Network Drive" is a unique location assigned to an individual custodian to store files. The Parties will search for responsive, relevant, non-privileged documents in the Network Drive (if any) assigned to each Custodian.

4. Desktop Work Stations, Laptops, and other devices

The Parties will use to the Search Terms to search the desktop work stations, laptops (if any), company-issued mobile devices (if any), and other devices (if any) of the Custodians identified in **Exhibit B**, for responsive, relevant, non-privileged documents stored locally as user-created files, unless a Party knows that documents stored locally will be duplicative of other documents produced.

5. Non-Custodial Data Sources Such as “Shared Drives,” “e-Rooms,” “Sharepoint” Sites, Lotus Notes Databases, Outlook Public Folders, etc.

Each Party has disclosed a list of non-custodial data sources (*e.g.* shared drives, servers, etc.), if any, likely to contain discoverable ESI, in **Exhibit C** to this ESI Protocol. The Parties will search for responsive, relevant, non-privileged documents saved as user-created files on the non-custodial data sources identified in **Exhibit C** to this ESI Protocol.

6. Additional Data Sources

The Parties will use the Search Terms to search for responsive, relevant, non-privileged documents saved as user-created files on external hard drives, portable media (such as flash drives, thumb drives, CD/ROMs and DVDs), and any other data storage devices utilized in the work environment to the extent they are identified by Custodians as likely to contain responsive, relevant information that is not stored in another data source identified above.

(b) Temporal Scope of Discovery

Document discovery will be limited to ESI and hard copy documents in the Parties’ custody, possession, or control last modified between November 1, 2020 and the present, to the extent such data currently exists.

As used in this ESI Protocol, the term “last modified” means as follows:

1. Email: the date and time sent based upon message level metadata;
2. ESI other than email: the later of the date populated in the “DateModified” metadata field, or if no “DateModified” is present in the metadata, the “DateCreated” metadata field, or, if neither such field is present, then the “ItemDate” metadata field;
3. Hard copy documents: the last known date of any modifications to the document (such as handwritten comments), or, if the modification date is

unknown, the creation date of the document, if known; provided, however, that if it is evident that a prior or original version of a modified hard copy document exists, then such document shall also be produced, even if such prior or original document falls without the time frame specified above. In the event that such prior or original version of a modified hard copy document does not appear in the hard copy documents collected by the Party and the receiving Party requests a further search to determine if such document exists, the Parties shall meet and confer regarding whether a further search to determine the existence of such a document is proportional to the needs of the case. In the event that the Parties cannot agree regarding whether a new search must be made for such prior or original version, either Party may apply to the Court for relief.

(c) Form of Production

The production format details specified by the Parties for their respective productions are found in **Exhibit D**.

(d) Deduplication

The Parties shall make reasonable efforts to deduplicate ESI. To the extent reasonably practicable, ESI shall be deduplicated across Custodians. ESI will be considered duplicative if it has the same content including metadata. For example, duplicates would include copies of the same electronic file saved on the local hard drives and/or network shared drives of multiple Custodians, even if different instances of the file reflect different dates created.

(e) Email Threading

To reduce the volume of entirely duplicative content within email threads, the Parties may utilize “email thread suppression.” As used in this agreement, email thread suppression means reducing duplicative production of email threads by producing the most recent email containing the thread of emails, as well as all attachments (excluding any hyperlinks) within the thread, and excluding emails constituting exact duplicates of emails within the produced string. For purposes of this paragraph, only email messages in which the parent document, senders and recipients, and all attachments are exactly the same will be considered duplicates.

(f) Foreign Language

All documents shall be produced in their original language. Where a requested document exists in a foreign language and the producing Party also has an English-language version of that document that it prepared for non-litigation purposes prior to filing of the lawsuit, the producing Party shall produce both the original document and all English-language versions. In addition, if the producing Party has a certified translation of a foreign-language document that is being produced (whether or not the translation is prepared for purposes of litigation), the producing Party shall produce the original document and the certified translation. Nothing in this agreement shall require a producing Party to prepare a translation, certified or otherwise, for foreign language documents that are produced in discovery

(g) Privileged Material

With respect to privileged or work-product information modified after April 2, 2025, the Parties are not required to include any such information in privilege logs.

The Parties agree that privilege logs shall include a unique identification number for each document and the basis for the claim (attorney-client privileged or work-product protection). For ESI, the privilege log may be generated using available metadata, including author/recipient or to/from/cc/bcc names; the subject matter or title and date created. Should the available metadata provide insufficient information for evaluating the privilege claim asserted, the producing Party shall include such additional information as required by the Federal Rules of Civil Procedure.

(5) No Waiver of Privileges or Immunities

Nothing in this ESI Protocol shall require production of information that a Party contends is protected from disclosure by the attorney-client privilege, the work-product doctrine, the common interest privilege, or any other privilege, doctrine, right, or immunity. Pursuant to Federal Rule of Evidence 502(d), the Parties acknowledge and agree that the inadvertent production of a privileged or work-product protected document is not a waiver of privilege or protection from discovery in this case or in any other federal or state proceeding where:

(1) the disclosure is inadvertent;

(2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and

(3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B).

A producing Party may assert privilege or work-product protection over produced documents at any time by notifying the receiving Party in writing of the assertion of privilege or protection. In addition, documents or information that contains privileged matter or attorney work-product shall be immediately returned to the procuring Party if such documents or information on their face appear to the receiving Party to have been inadvertently produced. The receiving Party may thereafter seek re-production of any such documents or information pursuant to applicable law.

(6) Processing Specifications

The producing Party shall use the following specifications when converting ESI from its native format into TIFF image or PDF files prior to production:

All tracked changes shall be maintained and displayed, to the extent reasonably feasible upon collection, so that all non-privileged changes to a document are evident.

To the extent practicable, consistent with reasonable production processes, attachments will be number stamped in sequence, after the document to which they were attached.

Author comments and presenter/speaker notes shall remain or be made visible, to the extent reasonably feasible upon collection.

(7) Third-Party ESI

Each Party has disclosed a list of third-party data sources, if any, that may contain discoverable ESI (e.g. third-party email and/or mobile device providers, "cloud" storage, etc.). These disclosures are included as **Exhibit E** to this ESI Protocol. Each Party has access to ESI stored with its respective, disclosed third-party data sources.

A Party that issues a non-party subpoena (the "Issuing Party") shall include a copy of this ESI Protocol with the subpoena and state that the Parties to the litigation have requested that third-parties produce documents in accordance with the specifications set forth herein.

The Issuing Party is responsible for producing any documents obtained under a subpoena to the other Party. If the Issuing Party receives any hard-copy documents or native files, the Issuing Party will process the documents in accordance with the provisions of this ESI Protocol, and then produce the processed documents to the other Party. However, any documents the Issuing Party does not intend to process for its own use may be disseminated to all the other Parties in the format in which such documents are received by the Issuing Party. If the Issuing Party subsequently processes any such documents, the Issuing Party will produce those processed documents to the other Party.

If the non-party production is not Bates-stamped, the Issuing Party will endorse the non-party production with unique prefixes and Bates numbers prior to producing them to the other Party.

(8) General Provisions

Third-Party Software. To the extent that documents produced pursuant to this ESI Protocol cannot be rendered or viewed without the use of proprietary third-party software, the Parties shall meet and confer to minimize any expense or burden associated with producing such documents in an acceptable format, including issues that arise with respect to obtaining access to any such software and operating manuals, which are the property of a third party.

This ESI Protocol shall have no effect on any producing Party's right to seek reimbursement for recoverable costs associated with collection, review, or production of documents or ESI.

Nothing in this ESI Protocol shall supersede the provisions of the any protective order entered in this action.

Nothing in this ESI Protocol shall be interpreted to require disclosure of irrelevant information or relevant information protected by the attorney-client privilege, work-product doctrine, or any other applicable privilege or immunity. The Parties do not waive any objections as to the production, discoverability, admissibility, or confidentiality of documents and ESI.

Each Party reserves the right to object to and challenge the data collection methodology utilized by the other Party.

Nothing in this ESI Protocol is intended or should be interpreted as narrowing, expanding, or otherwise affecting the rights of the Parties or third parties to object to a subpoena.

Dated: New York, New York
July 25, 2025

DAVIS WRIGHT TREMAINE LLP	EPSTEIN DRANGEL LLP
By:__/s John Magliery___________	By:___/S Kerry B. Brownlee
John M. Magliery Adam Sgro Francesca Reifer	Kerry B. Brownlee Jason M. Drangel Jodi-Ann McLane (admission

1251 Avenue of the Americas, 21st Floor
New York, NY 10020-1104
212-489-8230
johnmagliery@dwt.com
adamsgro@dwt.com
francescareifer@dwt.com

Attorneys for Plaintiff Interwork Korea Co., Ltd.

pending)
60 East 42nd Street, Suite 1250
New York, NY 10165
(212) 292-5390
jdrangel@ipcounselors.com
kbrownlee@ipcounselors.com
jmclane@ipcounselors.com

Attorneys for Defendant Lashify, Inc.

Date: July 28, 2025
New York, NY

SO ORDERED

ROBYN F. TARNOFSKY
UNITED STATES MAGISTRATE JUDGE

EXHIBIT A

INACCESSIBLE ESI

IWK:

1. None.

Lashify:

1. None, other than the email account of Jia Lin, which was deleted in or about October 2021.

EXHIBIT B

CUSTODIANS

IWK Custodians:

1. Hyunmyung Moon
2. Sangcheol Kwak
3. Seoin Yun
4. Jonghoon Lee
5. Nayeon Kim
6. Suzy Park
7. Changsoo Moon

Lashify Custodians:

1. Sahara Lotti
2. Jia Lin (to the extent documents remain in Lashify's possession, custody or control)[1]
3. Amie Jatana (Lashify email account only)
4. Kaarin Lanyi

[1] Jia Lin is no longer an employee of Lashify and in or about October 2021, her email account was deleted, although attachments and folders were migrated over. To the extent that any such attachments or folders remain in Lashify's possession, custody or control, they will be searched.

EXHIBIT C

NON-CUSTODIAL DATA SOURCES

IWK:

1. KakaoTalk
2. WhatsApp
3. Flow
4. WeChat

Lashify:

1. Google Drive;
2. Monday.com;
3. Air;
4. Dropbox;
5. Slack; and
6. OneDrive.

EXHIBIT D

PRODUCTION SPECIFICATIONS

To the extent reasonably practicable, the Parties shall produce documents in the following manner. If any Party is unable to do so, the Parties shall negotiate in good faith regarding the same:

1. Images:

- Produce documents 300 DPI, Single Page, black and white TIFF files (Gray Scale for .ppt files converted to TIFF), CCITT Group IV (2D Compression), or single page color JPG files
- Image Resolution at least 300 DPI
- Black and White unless Color or Gray Scale is necessary to understand the meaning
- File Naming Convention: Match Bates Number
- All TIFF image files shall be stored with a ".tif" extension
- All JPG files shall be stored with a ".jpg" extension
- No image folder shall contain more than 1,000 images
- Insert Placeholder image for files produced in native form (see Section V)
- Original document orientation shall be retained

2. Full Text Extraction / OCR:

- Produce full extracted text for all file types of ESI (redacted text will not be produced; OCR will be provided for redacted documents); produce OCR for hard copy documents or any documents where the extracted text was not fully recoverable
- Production format: Multi-page UTF-8 text files
- File Naming Convention: Text file names must be identical to the document identifier in the DAT file

3. LOAD FILE SPECIFICATIONS:

- Images Load File: Opticon OPT file, an image level comma-delimited file containing four fields per line: PageID,VolumeLabel,ImageFilePath,DocumentBreak

1) PageID – PageID of the item being loaded. MUST be identical to the image name (less the file extension). PageID must also be the same as ProdBeg/BegBates of each production
2) VolumeLabel – Optional. If used it is preferable that it match the VOLUMENAME assigned in the corresponding metadata load file.
3) ImageFilePath – The path to the image from the root of the delivery media.
4) DocumentBreak – The letter "Y" denotes the first page of a document. If this field is blank the page is not the first page of a document.

Example – ABC-JD00030005,ABC002,\ABC002\Images\001\ ABC-JD-00030005.tif,Y,,,

- Metadata/DAT Load File: Concordance DAT file containing delimited text that will populate fields in a searchable, flat database environment. ASCII text delimited load files defined using the following delimiters:

Field Separator	¶	ASCII 020
Text Qualifier	þ	ASCII 254
Substitute Carriage Return or New Line in Data	®	ASCII 174

- The first row of each metadata load file should be a header row containing the field names.
- All requested fields should be present in the metadata load file whether data exists or not.
- The text/DAT load file should also contain links to applicable native files, such as Microsoft Excel or PowerPoint files.
- The text/DAT file should also contain links to the OCR or Extracted Text files. Do not include the text in the load file.
- There should be one line for every record in the collection.
- The load file must contain a field map/key listing the metadata/database fields in the order they appear within the data file. For example, if the data file consists of a First Page of a Record (starting Bates), Last Page of a Record (ending Bates), DocumentID, Document Date, File Name, and a Title, then the structure may appear as follows:

þ BEGDOC þ ¶ þ ENDDOC þ ¶ þ DOCID þ ¶ þ DOCDATE þ ¶ þ FILENAME þ ¶ þ TITLE þ

- Extracted TEXT: Reference File Path to TEXT file in DAT file
- Native Files Produced: Reference File Path to Native file in DAT file

4. **ESI Production Metadata Fields** (slight name variations are permissible to correspond with the naming convention used in the review platform used by each Party):

- ProdBeg: Beginning Bates Number
- ProdEnd: Ending Bates Number
- ProdBegAttach: Beginning Bates number of the first document in an attachment range
- ProdEndAttach: Ending Bates number of the last document in attachment range
- Custodian: Name of the Custodian of the File(s) Produced – Last Name, First Name format
- DocExt: Document Extension is the File extension of the native file.
- FileName: Filename of the original digital file name
- Filesize: Size of native file, in bytes
- EmailSubject: Subject line extracted from an email message
- Title: Title field extracted from the metadata of a non-email document
- Author: Author field extracted from the metadata of a non-email document
- From: From field extracted from an email message
- To: To or Recipient field extracted from an email message
- Cc: CC or Carbon Copy field extracted from an email message
- BCC: BCC or Blind Carbon Copy field extracted from an email message
- Conversation Index: E-mail thread identification created by the e-mail system

- DateRcvd: Received date of an email message (mm/I/yyyy format)
- DateSent: Sent date of an email message (mIdd/yyyy format)
- DateCreated: Date that a file was created Im/dd/yyyy format)
- DateModified: Date of last modification of a document
- ItemDate: multi-purpose date field which reflects the sent date of an email message, and the last modification date, or the date of creation if the last modification date is not available, of a non-email document
- Fingerprint: MD5 or SHA-1 has value generated by creating a binary stream of the file
- ProdVolume: Identifies production media deliverable
- Redacted: "Yes," for redacted documents; otherwise, blank
- TimeRcvd: Time the e-mail message was received in the particular time zone of the Custodian
- TimeSent: Time the e-mail message was sent in the particular time zone of the Custodian
- TimeCreated: Creation time of the native file
- TimeModified: Time of last modification of a non-email document
- Confidentiality: Confidentiality designation of the produced record
- Record Type: i.e. E-DOC, Email, EmailAttach
- NativePath: Path and filename to produced Native file
- ExtractedText: File path to Extracted Text/OCR File
- OriginalFolderPath: The original source path/folder for each native document
- DUPE_Custodian: Custodian names from where the duplicates were removed based on global de-duplication

5. Paper Documents Metadata Fields:

- ProdBeg: Beginning Bates Number
- ProdEnd: Ending Bates Number
- ProdBegAttach: Beginning Bates number of the first document in an attachment range
- ProdEndAttach: Ending Bates number of the last document in attachment range
- Custodian: Name of the Custodian of the File(s) Produced – Last Name, First Name format
- ProdVolume: Identifies production media deliverable
  - Pages: The number of imaged pages per document i.e. Page count
  - Redaction: "Yes," for redacted documents; otherwise, blank
  - Confidentiality: Confidentiality designation of the produced record
  - ExtractedText: File path to Extracted Text/OCR File

<u>PRODUCTION FORMAT</u>

1. Document Image Format

Paper documents and ESI shall be produced in Tagged Image File Format ("TIFF"). Specifically, documents shall be produced as 300 D.P.I. Group IV compression black and white single-page TIFF images, with original document orientation retained, subject to the following exceptions.

a. Native Format

i. ESI that cannot be converted to TIFF format (video files or audio files), documents without standard pagination, such as spreadsheets (including Microsoft Excel) or desktop databases (such as Microsoft Access), and other file formats, files or documents that are too large to be practically converted to TIFF format or that do not render well to TIFF format, will be produced in native format with a TIFF placeholder identifying that the document was produced natively.

ii. Each Party reserves the right to request native files for documents that are difficult to understand after they have been produced in TIFF format or that contain potentially relevant embedded information, and such requests will not be unreasonably denied. Within fourteen (14) days of receiving such a request, the producing Party will either produce the requested native files or respond in writing, setting forth its position on the production of the requested documents. If the Parties are unable to agree as to the production of the requested documents in native format, the Parties may submit the matter to the Court for resolution.

iii. Notwithstanding anything to the contrary in this ESI Protocol, redacted documents will not be produced in native format.

b. Color Images

A Party shall produce color images for a reasonable number of selected documents if requested to do so in writing by the receiving Party. If requested, color images should be delivered in JPG format. Notwithstanding the foregoing, scanned or digital photographs which exist natively as color images shall be produced as color images, not black and white images.

3. Naming of Files

a. File Name for Images

Each document image file shall be named with the unique Bates Number, or the unique beginning Bates number in the case of a multi-page document. The Bates Number for documents produced by IWK shall begin with the prefix “IWK.” The Bates Number for documents produced by Lashify shall begin with the prefix “LASHIFY.” Further, each unique Bates Number for that document shall be electronically “burned” into the image at a place on the document that does not obscure, conceal or interfere with any information originally appearing on the document. File names should not contain embedded spaces, hyphens, commas, underscores, ampersands, slashes, back slashes, hash marks, plus signs, percent signs, exclamation marks, any character used as a delimiter in the metadata load files, or any character not allowed in Windows file-naming convention.

b. File Name for Native Files

When producing a file in native format, the native file shall be named with the Bates number and confidentiality designation (if any) as the file name, and it shall be accompanied by a TIFF image marked with the words “File Produced Natively”.

4. Document Unitization

If a document is more than one page, the Parties shall make reasonable efforts, consistent with reasonable production practices, to provide the logical unitization of the document and any attachments and/or affixed notes as they existed in the original document.

5. Searchable Text

In addition to TIFF images, each production will include multi-page text files corresponding to the TIFF files described above.

a. <u>Hard Copy Documents</u>

Hard copy documents shall be scanned using Optical Character Recognition ("OCR") technology, and a single searchable ASCII (".txt") file shall be produced for each document. Each file shall be named with the unique Bates Number of the corresponding TIFF document followed by the extension ".txt".

b. <u>Electronic Documents</u>

The full text of each native electronic document shall be extracted ("Extracted Text") and produced in a text (".txt") file. The Extracted Text shall be provided in searchable ASCII text format and shall be named with the unique Bates Number of the corresponding TIFF document followed by the extension ".txt". However, documents that were images in their native form (*e.g.*, PDF and TIFF) or otherwise do not have searchable text in their original form will be produced as TIFF images without searchable text. Each Party will make reasonable efforts to obtain text files via OCR if no extractable text is available.

c. <u>Redacted Documents</u>

Documents produced with redactions shall be scanned using OCR technology, and a single searchable ASCII text format file shall be produced for each document. Each file shall be named with the unique Bates Number of the corresponding TIFF document followed by the extension ".txt".

d. <u>Text File Format</u>

All soft and hard returns in the native electronic or image file should be replicated as a carriage return and line feed ("CRLF") in the text file (*i.e.*, the lines of text in the file terminate with a CRLF in correlation with the appearance of the native electronic or rendered image file). Multi-line paragraphs of emails should not be rendered as a single, extended line of text. Text files should include page breaks that correspond to the pagination of the image files.

6. Production Media

Documents shall be made available to the other Party by file transfer protocol (FTP) or other secure, password-protected file-sharing system (the "Production Media"), and will include .dat and .opt load files.

7. Folders on the Production Media

Each production of documents shall contain one or more folders containing the image files, with the number of image files limited to 1,000 per folder. Images for a given document must reside together in the same folder. The maximum number of native files in a subfolder should be limited to 1,000 per folder. Text files containing the searchable text for all scanned hard copy and electronic documents should be placed under a “FULLTEXT” or “TEXT” folder, with a Control List file for loading placed in the “LOADFILES” or “DATA” folder on the delivery media.

8. ESI Production Metadata Fields and Hard Copy Load File Fields

In connection with the production, the Parties agree to produce the metadata and hard copy load file fields, to the extent data exists for any such field, that are set forth in the “PRODUCTION SPECIFICATION” section of this Exhibit.

9. Original Documents

Nothing in this ESI Protocol shall eliminate or alter any Party’s obligation to retain native format copies, including associated metadata, of all ESI produced in this litigation and original documents produced in this litigation which originated as hard copy documents.

10. De-Duplication, De-NISTing, Parent/Child Integrity

A Party is only required to produce a single copy of a responsive document. Parties may de-duplicate stand-alone documents or entire document families globally using MD5 or SHA-1 Hash Value matching. ESI that is not an exact duplicate may not be removed. Common system files defined by the NIST library (http://www.nsrl.nist.gov/) need not be produced. Attachments to emails shall not be eliminated from the parent email, with the exception of inline image attachments less than 15 KB, or otherwise identified through manual review, to avoid repetitive email signature images. Paper documents shall not be eliminated as duplicates of responsive ESI. To the extent the Parties de-duplicate stand-alone electronic documents against an e-mail attachment, the attachment to the e-mail must be the document that is produced.

EXHIBIT E

THIRD-PARTY ESI

IWK:

1. None.

Lashify:

None, other than non-custodial sources, which Lashify has access to.